

1. A method for encrypting a digital image comprising:

```
5      partitioning the unencrypted image into at least one
      partition;
```

applying a second S box to each partition;

2. The method according to Claim 1, wherein  
providing the unencrypted image comprises generating the  
15 unencrypted image at a camera.

3. The method according to Claim 1, wherein the unencrypted image comprises an image portion and a text portion and wherein partitioning the unencrypted image comprises:

partitioning the image portion into at least one  
e partition blocks based on a minimum partition block  
and a maximum partition block size;

indexing the text partition blocks.

4. The method according to Claim 3, wherein the minimum partition block size is less than a length of a

cryptographic key and the maximum block size is less than the length of the cryptographic times the dimensionality of a product space associated with the second S box.

5           5. The method according to Claim 1, wherein applying the P box comprises:

          applying a bit enumeration to each partition;  
          permuting a plurality of bits in each partition; and  
          rotating a plurality of nibbles in each partition.

10

          6. The method according to Claim 1, wherein applying the first S box comprises:

          applying a first non-linear feedback shift register to the partition;

15

          selecting a nibble from the partition;

          comparing the selected nibble against an entry in a predetermined table;

          modifying the nibble based on the comparison;

          applying a second nonlinear feedback shift register

20

to the partition;

          applying a rotation matrix to at least one of the nibbles in the partition; and

          determining whether a predetermined number of twiddles has been applied to the partition.

25

          7. The method according to Claim 6, wherein the first non-linear feedback shift register comprises a non-linear feedback shift register number three and the second non-linear feedback shift register comprises a  
30 non-linear feedback shift register number four.

10028017-122101

8. The method according to Claim 1, wherein the second S box comprises:

determining a trajectory associated with each partition; and

5 determining a ring associated with each trajectory.

10028017-122101

9. A method for digital image decrypting comprising:

providing an encrypted digital image;  
reconstruct at least one partition based on the  
5 encrypted digital image;  
reconstruct at least one trajectory associated with  
the encrypted digital image;  
applying a reverse S2 box to the partitions based on  
the trajectories;  
10 applying a reverse S1 box to the partitions;  
applying a reverse P box to the partitions; and  
generating an unencrypted digital image based on the  
first reverse S box, the second reverse S box and the  
reverse P box.

15 10. The method according to Claim 9, wherein  
reconstructing at least one trajectory comprises:

determining a set of at least one possible  
trajectory;  
20 applying an S2 box to each possible trajectory in  
the set to generate an encrypted possible trajectory;  
comparing the encrypted possible trajectory to the  
encrypted digital image; and  
determining at least one actual trajectory when the  
25 comparison finds a match.

11. The method according to Claim 9, wherein  
applying the reverse S1 box comprises:

applying a rotation matrix to at least one of the  
30 nibbles in the partition  
applying a second nonlinear feedback shift register  
to the partition

1002807-122101

selecting a nibble from the partition;  
comparing the selected nibble against an entry in a  
predetermined table;  
modifying the nibble based on the comparison; and  
5       applying a first non-linear feedback shift register  
to the partition.

12. The method according to Claim 11, wherein the  
first non-linear feedback shift register comprises a non-  
10       linear feedback shift register number three and the  
second non-linear feedback shift register comprises a  
non-linear feedback shift register number four.

13. The method according to Claim 9, wherein  
15       applying the reverse P box comprises:  
rotating a plurality of nibbles in each partition;  
permuting a plurality of bits in each partition; and  
applying a bit enumeration to each partition.

14. The method according to Claim 9, wherein  
20       applying the reverse S2 box comprises:  
determining a ring associated with each trajectory;  
and  
25       determining a trajectory associated with each  
partition.

10023017-122001

15. A system for encrypting a digital image comprising:

software stored in memory and operable to:

provide an unencrypted image;

5 partition the unencrypted image into at least one partition;

apply a P box to each partition;

apply a first S box to each partition;

apply a second S box to each partition; and

10 generate an encrypted image based the P box, the first S box and the second S box.

16. The system according to Claim 15, wherein the software is further operable to generate the unencrypted  
15 image at a camera.

17. The system according to Claim 15, wherein the unencrypted image comprises an image portion and a text  
portion and wherein the software is further operable to:

20 determine a dimension of the unencrypted image;

partition the image portion into at least one image partition blocks based on a minimum partition block size and a maximum partition block size;

25 partition the text portion into at least one text partition blocks based on the minimum partition block size and the maximum partition block size;

index the image partition blocks; and

index the text partition blocks.

30 18. The system according to Claim 17, wherein the minimum partition block size is less than a length of a cryptographic key and the maximum block size is less than

10028037-122101

the length of the cryptographic times the dimensionality of a product space associated with the second S box.

19. The system according to Claim 15, wherein the  
5 software is further operable to:

apply a bit enumeration to each partition;  
permute a plurality of bits in each partition; and  
rotate a plurality of nibbles in each partition.

10 20. The system according to Claim 15, wherein the software is further operable to:

apply a first non-linear feedback shift register to the partition;

select a nibble from the partition;

15 compare the selected nibble against an entry in a predetermined table;

modify the nibble based on the comparison;

apply a second nonlinear feedback shift register to the partition;

20 apply a rotation matrix to at least one of the nibbles in the partition; and

determine whether a predetermined number of twiddles has been applied to the partition.

25 21. The system according to Claim 20, wherein the first non-linear feedback shift register comprises a non-linear feedback shift register number three and the second non-linear feedback shift register comprises a non-linear feedback shift register number four.

30

22. The system according to Claim 15, wherein the software is further operable to:

10026017-122101

determining a trajectory associated with each  
partition; and

determining a ring associated with each trajectory.

100221-100200



23. A method for digital image decrypting comprising:

providing an encrypted digital image;  
reconstruct at least one partition based on the  
5 encrypted digital image;  
reconstruct at least one trajectory associated with  
the encrypted digital image;  
applying a reverse S2 box to the partitions based on  
the trajectories;  
10 applying a reverse S1 box to the partitions;  
applying a reverse P box to the partitions; and  
generating an unencrypted digital image based on the  
first reverse S box, the second reverse S box and the  
reverse P box.

15 24. The method according to Claim 23, wherein  
reconstructing at least one trajectory comprises:  
determining a set of at least one possible  
trajectory;  
20 applying an S2 box to each possible trajectory in  
the set to generate an encrypted possible trajectory;  
comparing the encrypted possible trajectory to the  
encrypted digital image; and  
determining at least one actual trajectory when the  
25 comparison finds a match.

25. The method according to Claim 23, wherein  
applying the reverse S1 box comprises:  
applying a rotation matrix to at least one of the  
30 nibbles in the partition  
applying a second nonlinear feedback shift register  
to the partition

10026017.122101

selecting a nibble from the partition;  
comparing the selected nibble against an entry in a  
predetermined table;  
modifying the nibble based on the comparison; and  
5       applying a first non-linear feedback shift register  
to the partition.

26. The method according to Claim 25, wherein the  
first non-linear feedback shift register comprises a non-  
10   linear feedback shift register number three and the  
second non-linear feedback shift register comprises a  
non-linear feedback shift register number four.

27. The method according to Claim 23, wherein  
15   applying the reverse P box comprises:  
rotating a plurality of nibbles in each partition;  
permuting a plurality of bits in each partition; and  
applying a bit enumeration to each partition.

28. The method according to Claim 23, wherein  
20   applying the reverse S2 box comprises:  
determining a ring associated with each trajectory;  
and  
determining a trajectory associated with each  
25   partition.

10023017-122101

29. A system for encrypting a digital image comprising:

means for providing an unencrypted image;

means for partitioning the unencrypted image into at

5 least one partition;

means for applying a P box to each partition;

means for applying a first S box to each partition;

means for applying a second S box to each partition;

and

10 means for generating an encrypted image based the P box, the first S box and the second S box.

10028017-122101

30. A system for digital image decrypting comprising:

- means for providing an encrypted digital image;
- 5 means for reconstruct at least one partition based on the encrypted digital image;
- means for reconstruct at least one trajectory associated with the encrypted digital image;
- means for applying a reverse S2 box to the
- 10 partitions based on the trajectories;
- means for applying a reverse S1 box to the partitions;
- means for applying a reverse P box to the partitions; and
- 15 means for generating an unencrypted digital image based on the first reverse S box, the second reverse S box and the reverse P box.

20250317 12:10:11